DATE(S) ISSUED:

9/10/2013

SUBJECT:

Multiple Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS13-072)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office that could result in remote code execution. Exploitation may occur if a user opens a specially crafted Office file using an affected version of Microsoft Office. Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Twelve memory corruption vulnerabilities have been identified in Microsoft Office that could allow remote code execution. One vulnerability has been identified in Microsoft Word that could allow information disclosure. These vulnerabilities are caused due to the way that Microsoft Office handles specially crafted files.

- Multiple Memory Corruption Vulnerabilities in Microsoft Word (CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3850, CVE-2013-3851, CVE-2013-3852, CVE-2013-3853, CVE-2013-3854, CVE-2013-3855, CVE-2013-3856, CVE-2013-3857, CVE-2013-3858)
- XML External Entities Resolution Vulnerability (CVE-2013-3160)

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose

accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider viewing emails in plain text.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms13-072

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3160

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3847

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3848

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3849

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3850

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3851

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3852

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3853

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3854

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3855

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3856

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3857

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3858